



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/669,352	09/26/2000	Stephen A. Bagshaw	ATI000092	4574

34456 7590 01/14/2005
TOLER & LARSON & ABEL L.L.P.
5000 PLAZA ON THE LAKE STE 265
AUSTIN, TX 78746

EXAMINER

HO, THOMAS M

ART UNIT PAPER NUMBER

2134

DATE MAILED: 01/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Applicati n No.

09/669,352

Applicant(s)

BAGSHAW, STEPHEN A.

Examin r

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 8/06/04.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 7, 10-20, 24-32 and 35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 7, 10-20, 24-32 and 35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-35 are pending.

Response to Arguments

2. Applicant's arguments, see pgs 7-8, filed 1/8/04, with respect to the rejection(s) of claim(s) 1-9, 12-16, 21-23 under 35 USC 102(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of 35 USC 102(e).

Applicant has objected to Examiner's characterization of the A-key of Patel as a public key. One of ordinary skill in the art will recognize that a public encryption key is one encryption key of a key pair that may be provided via non-secure means since the public key encryption key is used only to encrypt information.

The Examiner would contend however, that the public and private keys are merely labels, flexible to a variety of different uses, as essentially, the keys are only digital bits of information. For Example, the Applicant asserted above that the public encryption key is used **only** to encrypt information but then proceeds in claim 1 to use the public key to generate a second seed key rather than encrypt information.

Art Unit: 2134

While Applicant objects to Examiner's characterization of the A-key as a public key, the Examiner contends Applicant himself does not adhere to the strict interpretation of a public key.

A key is only a digital string of information consisting of zeroes and ones, capable of being used in any manner that digital information is used, namely because a key *is* digital information. For this reason, in the following rejection below, the Examiner has interpreted the A-key to be a public key.

Applicant has also objected to Patel (Column 4, lines 1-11) in that no key appears to be provided, nor does there appear to be any hardware controller disclosed.

The Examiner notes however, that applicant's objections are inherent to Patel. When a key is generated, that key is in some sense, "provided". Additionally, the generation of a key in Patel inherently discloses a hardware controller to at least perform the generation. A key cannot be generated unless there is at least a physical mass to perform the generation.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted

Art Unit: 2134

on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5, 7, 12-16, are rejected under 35 U.S.C. 102(e) as being anticipated by Patel, US Patent 6,243,811.

In reference to claim 1:

Patel (Column 4, lines 1-11) discloses a method comprising:

- Establishing an encrypted link between a peripheral device and a software component of an information handling system, wherein establishing the encrypting link includes generating a first seed key common to both the peripheral device and the software component., where the peripheral device is the mobile unit, the software component of the information handling system is the software of the AC, the first seed key is M-Key, which is common to both the mobile unit and the AC.
- Providing the first seed key and a public encryption key associated with the peripheral device to a hardware controller, where the public encryption key is the A-key which is unique to the hardware controller, the HLR, and the peripheral, the mobile. (Column 4, lines 1-11)
- Generating in the hardware controller, using the first seed key and the public encryption key, a second seed key different from the first seed key, the second key to encrypt communications between the software component and the

Art Unit: 2134

hardware controller, where the SSD generated is the second seed key generated from the A-key and the M-key. (Column 1, lines 55-64)

In reference to claim 2:

Patel(Column 4, lines 1-4) discloses a method wherein generating the first seed key is performed by the software component, where the software component is the software that executes on the AC/HLR and where the first seed key is M-key.

In reference to claim 3:

Patel (Column 2, lines 22-30) discloses a method wherein generating the first seed key includes:

- Using the public encryption key(A-Key) associated with the peripheral device(the Mobile) to select a plurality of private encryption keys associated with the software component(AC/HLR), where the private encryption keys are SSDA and SSDB
- Determining the seed key based upon the selected private keys associated with the software component, where Patel discloses that the seed key SSD is based upon the selected private keys SSDA and SSDB.

In reference to claim 4:

Patel(Column 4, lines 1-4) discloses a method wherein generating the first seed key is performed by the peripheral device, where the peripheral device is the mobile, and the first seed key is the M-Key.

Art Unit: 2134

In reference to claim 5:

Patel (Column 2, lines 22-30) discloses a method wherein generating the first seed key includes:

- Using the public encryption key(A-Key) associated with the software component(AC/HLR) to select from a plurality of private encryption keys(SSDA, SSDB) associated with the peripheral device(The mobile);
- And summing the select private keys associated with the peripheral device, where SSDA and SSDB are combined.

In reference to claim 7:

Patel(Column 4, 51-62) & (Column 2, lines 56-57) discloses a method wherein including:

Providing the public encryption key(A-key) associated with the peripheral device(Mobile) and a private decryption key(SSDA), associated with the software component(AC/HLR software), to the hardware component(AC/HLR hardware);

Providing public key encryption between the hardware controller(HLR) and the peripheral device(Mobile), where the public key encryption is understood to be established between to AC/HLR and the mobile, as the purpose of Patel is to establish the keys to be used.

In reference to claim 12:

Patel(Column 1, lines 55-59) & (Column 4, lines 1-11) discloses a method wherein the step of establishing further includes the first seed key being based upon the peripheral

Art Unit: 2134

device and the information handling system, where the first seed key is based on the A-key, which is unique to the peripheral device and the information handling system.

In reference to claim 13:

Patel(Column 1, lines 55-59) & (Column 4, lines 1-11) discloses a method wherein the first seed key is unique to the peripheral device and the information handling system, where the first seed key is based on the A-key, which is unique to the peripheral device and the information handling system.

In reference to claim 14:

Patel discloses a hardware controller comprising:

- A bus connection to receive a first seed key(M-key) from a software component(software of the AC/HLR) within an information handling system(AC), where the M-key is received from the PRF function used to generate it. (Column 4, lines 1-10)
- A digital communications connector to connect to a peripheral device(mobile) and to receive a public encryption key from said peripheral device, where the digital communications connector allows for the wireless mobile connection.
- A first set of registers to store said first seed key, (M-key) said first seed key common to both said information handling system and the peripheral device, where the first register is the home location register, which acts as a communication conduit, or the Authentication Center. (Column 4, lines 1-11)

Art Unit: 2134

- A second register to store said public encryption key(A-key), where the second register is the Home location register. (Column 1, lines 55-59)
- A processing circuit to generate, using said first seed key and said public encryption key a second seed key different from said first seed key, said second seed key to encrypt communications between said software component and said hardware controller, where the SSD is used in the encrypted data between the mobile and the system. (Column 2, lines 55-59)

Claim 15 is rejected for the same reasons as claim 5.

In reference to claim 16:

Patel(Column 1, lines 40-48) discloses a hardware controller wherein communications between said hardware controller(HLR) and said information handling system(AC) are performed over a system bus, where a system bus is inherent to the information systems necessary to transmit information. Examiner further maintains that a system bus is inherent to all desktop computer systems today.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2134

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 10, 11, 17-20, 24-32, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel.

In reference to claim 10:

Patel discloses all of claim 10 except a method wherein the hardware controller is a video controller.

The examiner takes official notice that it was well known to those of ordinary skill in the art that a type of hardware controller is a video controller.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a video controller, in order to extend cryptographic communications to that type of hardware controller.

In reference to claim 11:

Patel discloses all of claim 11 except a method wherein the peripheral device is a display device.

The examiner takes official notice that a display device was a well known peripheral device at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a display peripheral device as a peripheral device, in order to extend cryptographic communications to that peripheral entity.

Art Unit: 2134

In reference to claim 17:

Patel discloses all of claim 17 except a hardware controller wherein said system bus is a peripheral component interconnected bus.

The examiner takes official notice that PCI buses were well known to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to disclose a system wherein the system bus was a PCI bus, to allow communications with other PCI devices.

In reference to claim 18:

Patel discloses all of claim 18 except a hardware controller wherein said digital communications connector is a digital video interface connector.

The examiner takes official notice that digital video interface connectors were a well known type of digital communications connector to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to disclose a system that used digital video interface connectors in order to extend digital communications to digital video.

Claim 19 is rejected for the same reasons as claim 10.

Claim 20 is rejected for the same reasons as claim 11.

In reference to claim 24:

Art Unit: 2134

Patel discloses a processor coupled to a system bus:

- A collection of instructions to be stored and executed by said processor, said collection of instructions including instructions to establish an encrypted link between said system and a peripheral device(Mobile), wherein establishing said encrypted link includes generating a first seed key(M-key) common to both said peripheral device and said system, said collection of instructions further including instructions to deliver said first seed key to a peripheral controller, where the collection of instructions is the software executed establishes an encrypted link between the AC/HLR and the mobile through a session request. (Column 2, lines 27-35) to generate a first seed key, M-key common to both the peripheral and the system. (Column 4, lines 1-11)
- A peripheral controller including a bus connection to receive said first seed key(M-key), where the communications controller on the mobile receives the seed key from the PRF function (Column 4, lines 1-11)
- A digital communications link to connect to said peripheral device and to receive a public encryption key (A-key) from said peripheral device(Mobile), where key is received by the mobile through manufacturing. (Column 1, lines 55-59)
- A first set of registers to store said first seed key(M-key), where the visiting location register may store the M-key because it acts as a conduit of communication between the system and the mobile, or the Authentication Center, another registry where the M-key must be stored. (Column 4, lines 12-19)
- A second register to store said public encryption key(A-key), where the second register is the Home location register. (Column 1, lines 55-59)

Art Unit: 2134

- A processing circuit to generate, using said first seed key(M-key) and said public encryption key, a second seed key(SSD) different from said first seed key, said second seed key to encrypt communications between said system and said peripheral controller (Column 2, lines 20-30)

Patel fails to explicitly disclose memory coupled to said system bus for use by said processor.

The examiner takes official notice that memory coupled to a bus for use by a processor was well known at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to couple memory to a system bus to a processor in order to allow the processor to access the memory.

In reference to claim 25:

Patel discloses all of claim 25 except a system wherein said memory includes random access memory and read-only memory.

The examiner takes official notice that systems which include RAM and ROM were well known to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to disclose a system that included RAM and ROM to allow the system to store data.

Claim 26 is rejected for the same reasons as claim 5.

Art Unit: 2134

In reference to claim 27:

Patel discloses a system wherein said public encryption key and said plurality of private encryption keys are located the mobile and the AC/HLR, and thereby inherently located in the memory of each device.

Claim 28 is rejected for the same reasons as claim 17.

Claim 29 is rejected for the same reasons as claim 18.

Claim 30 is rejected for the same reasons as claim 10.

Claim 31 is rejected for the same reasons as claim 11.

Claim 32 is rejected for the same reasons as claim 6.

In reference to claim 35:

Patel(Column 1, lines 55-60) discloses a system wherein the digital communications link is to receive a public encryption key from said peripheral device, where the peripheral device is the mobile, and to transmit encrypted digital data to said peripheral device, where the data transmitted the to the peripheral device is encrypted with session keys.
(Column 2, lines 55-58)

Conclusion

8. The following prior art not relied upon is made of record:

US Patent 6,173,174 is a method for updating SSD and A-key entries in Mobile telephones.

Art Unit: 2134

9. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

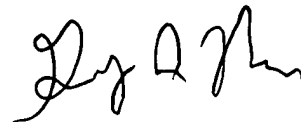
The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

January 8th 2005



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100